

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

White and rose color Apple iPhone model A1586 with IMEI
356153092554788, more fully described in Attachment A.

Case No. 19-M-1224

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

White and rose color Apple iPhone model A1586 with IMEI 356153092554788, more fully described in Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

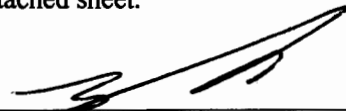
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. §§ 922(a)(6), 922(g)(3), and 371

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

TFO Rodolfo Ayala, ATF
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/14/19


Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William Duffin, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Rodolfo Ayala, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is described in paragraph seven below and in Attachment A and is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a state certified law enforcement officer currently assigned to the Milwaukee Police Department's Special Investigations Division-Alcohol, Tobacco, Firearms and Explosives Violent Impact Team. I investigate narcotics trafficking as well as individuals who possess firearms and are prohibited from doing so.

3. I have worked full-time as a law enforcement officer for the past 16 years. I have been a deputized, full time Task Force Officer ("TFO") with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") for the past nine years. I am currently assigned to the Chicago Field Division-Milwaukee III field office.

4. I have received training in the investigation of unlawful possession of firearms and possession of firearms by prohibited persons. I have received training in the investigations of Federal firearm and narcotic offenses, such as to, 18 U.S.C. § 922 (d)-knowing sale to a prohibited person; 18 U.S.C. § 922 (g)-knowing possession of firearm by prohibited person; and 26 U.S.C.,

5861 (d)-receipt or possession of unregistered firearm. I have worked with local, state and federal law enforcement agents investigating the possession, use, and trafficking of controlled substances and weapons in the Milwaukee area; I have participated in the execution of numerous search warrants in which weapons were seized; I am familiar with the different types and calibers of firearms and ammunition commonly possessed for illegal purposes; I am professionally trained in the use of firearms; I have conducted investigations involving the intentional transfer of a firearm from a non-prohibited person to a prohibited person; I have experience working with confidential informants, citizen informants, and sources of information.

5. The facts in this affidavit come from (1) my personal observations, training and experience, and (2) information obtained from other agents working on this investigation ("case agents"), witnesses, cooperating defendants, and confidential informants. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, and instrumentalities of violations of 18 U.S.C. §§ 922(a)(6), 922(g)(3), 371 are located in the Device for which authority is requested to search.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The property ("Device") to be searched is a White and Rose color Apple iPhone model A1586 with IMEI 356153092554788 and currently in the custody of ATF. The Device

was seized while executing an arrest warrant of Darius S. Hall on March 11, 2019, at 206 N. 37th St., Milwaukee, WI.

8. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

SUMMARY OF INVESTIGATION

9. On July 17, 2015, Darius Hall reported to the Milwaukee Police Department ("MPD") that he had a firearm (JGA Janine Pistol, 9mm) stolen from his girlfriend's unlocked car the day before. On February 7, 2016, the gun was recovered after it was thrown out of the window of a car in a high-speed pursuit.

10. On August 16, 2017, Darius Hall reported to MPD that another firearm (black, 9mm, Taurus) was stolen from an unlocked car two days before.

11. On March 14, 2018, Darius Hall reported to MPD that a different firearm (Springfield Arms 40 Cal.) that he owned was stolen from his girlfriend's (Angelique Bolden's) car. Bolden had purchased the gun initially, and Hall showed a notarized bill of sale indicating he bought the firearm for \$500 on September 12, 2017.

12. On January 9, 2019, at 10:36, there was a shots fired report. Several seconds later, Hall called the police to report that someone had stolen his 9mm Taurus handgun from an unlocked car approximately two blocks from the shooting. A 9mm shell was found on the scene of the shooting. MPD Officers arrived on scene 11 minutes later and Hall was not there. MPD Officers eventually interviewed Hall who described playing outside at a park at 10:30 p.m. in 20 degree weather with his three children who were the following ages: four months, just over one year, and almost six years old. He then said he came back to his car and determined that his gun was stolen.

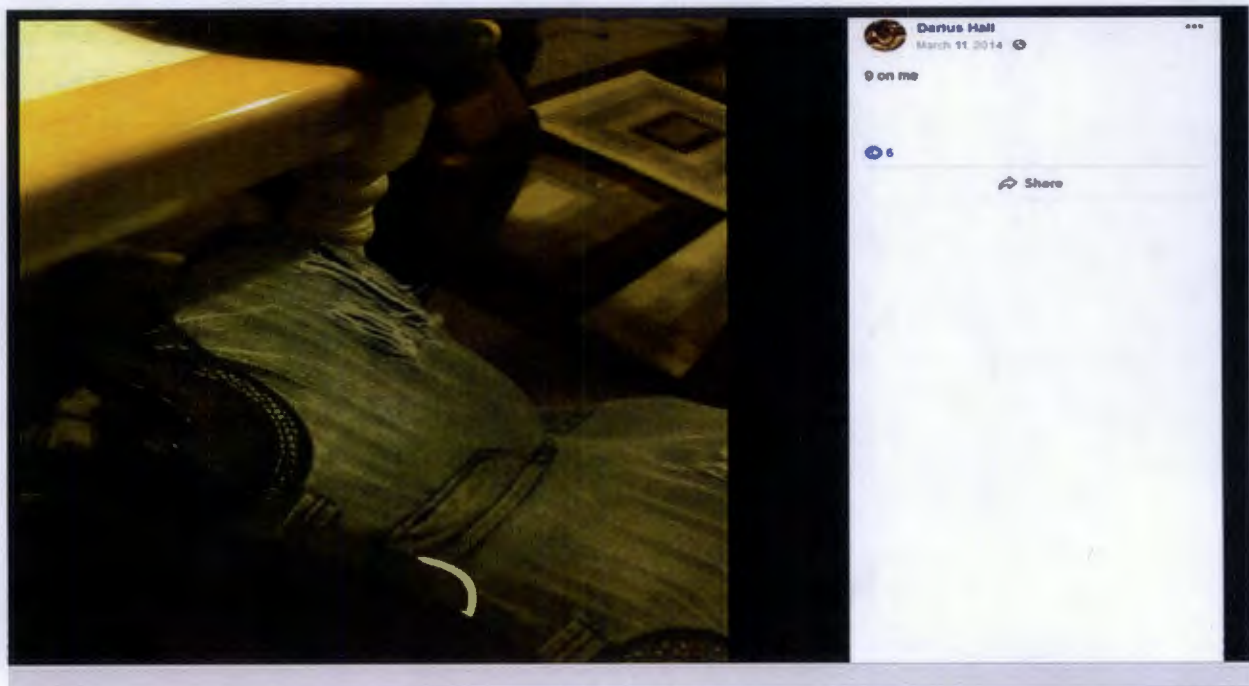
Later in the interview, he stated that the reason he left the scene was because he had to go pick up his girlfriend (Ms. Bolden) on the south side of Milwaukee. MPD Officers then interviewed Ms. Bolden who stated that she had been at her home (not on the south side, near the shooting) napping the whole evening. Hall was arrested for obstruction and questioned by police. During his questioning, he admitted that he has smoked marijuana every day since high school.

13. Based off of this incident, ATF began investigating Hall and learned that he had a child in common with an individual named A.T. who had filed a police report in which she reported that a firearm was stolen from her apartment in June of 2015 (Hi Point 9mm). Case agents interviewed A.T. and she admitted that she purchased the firearm for Hall, and once she picked it up, she gave it to Hall and never saw it again. In June of 2015, Hall then told her to file a false police report saying that the firearm was stolen. She then filed the false police report.

14. Case agents reviewed Hall's Facebook account and determined that on March 10, 2014, Hall posted a picture of himself with money, marijuana, and what looks to be a scale on Facebook:



15. The next day, he posted a picture of himself with a firearm that based on my training and experience I can identify as a Hi-Point 9mm (the type of and caliber of gun A.T. said she bought Mr. Hall):



16. On the same day, he also posted this on Facebook:



17. These pictures corroborate what A.T. told case agents (he looks to be possessing the firearm) and also provide a motive for wanting a firearm, and ideally a firearm in someone else's name—dealing drugs. At the time A.T. purchased the firearm for Hall, Hall was under 21 and not allowed to purchase a firearm from a federally licensed dealer.

18. On March 5, 2019, a grand jury sitting in the Eastern District of Wisconsin returned a three-count indictment against Hall alleging that he (1) aided and abetted A.T. in making a false statement to a federally licensed firearms dealer in violation of 18 U.S.C. 922(a)(6) & 2 on March 5, 2014; (2) conspired from February 2014 until at least January 9, 2019 to make false statements in connection with the acquisition of firearms from licensed dealers in violation of 18 U.S.C. §§ 922(a)(6) and 371; (3) unlawfully possessed a firearm on May 10, 2018 because he was an unlawful user of marijuana.

19. On March 11, 2019, at approximately 9:45 a.m., Special Agents and TFOs from ATF conducted a knock and talk at 206 N. 37th St., Milwaukee, Wisconsin. Angelique S. Bolden opened the door and advised officers that Hall was not home, but gave verbal consent for the officers to search her residence for Hall. Hall was located on the second floor, hiding under clothes in a bedroom closet. He did not have a phone on his person at that time. Hall was arrested.

20. While speaking with Bolden, I asked her for Hall's phone number. She then pulled out her phone and scrolled through her contacts and provided me with a phone number for Hall: (414) 722-0898. I observed Bolden's phone at that time and she had this number saved under a nickname for Hall that is consistent with the type of nickname one might give to a significant other. I then called the number ((414) 722-0898) and then observed the Device ringing in the living room. I grabbed the Device and observed my number on the screen. I then took possession of the Device. A few days earlier (March 7, 2019) case agents contacted a confidential source who verified that Bolden lists Darius Hall as an emergency contact at the above number in January of 2019. The Device is colloquially known as an iPhone 6 and was released by Apple in September of 2014.

21. Based on my training and experience, I know that individuals use their cell phones to obtain illegal drugs including marijuana. I also know that an individual who smokes marijuana every day for several years is likely to continue to smoke marijuana daily. In fact, when Hall was arrested on March 11, 2019, he submitted to a voluntary drug test in lockup and was positive for marijuana. Based on an ATF 4473 form, I know that on May 10, 2018, Hall picked up a Taurus G2C, 9mm pistol, bearing serial number TL081109 from a federally licensed firearm dealer. Based on the investigation to date, I know that Hall regularly possesses, sells, and purchases firearms. Based on what he reported to MPD, Hall possessed a firearm on January 9, 2019. Based on the investigation to date, Hall likely possessed other firearms from January 9, 2019 through

present. Accordingly, there is probable cause to believe that there is evidence and instrumentalities of 18 U.S.C. 922(g)(3)—unlawful user of a controlled substance in possession of a firearm on the Device.

22. Based on my training, experience, the investigation to date, and the number of police reports for stolen firearms Hall has filed, it is likely that Hall is obtaining firearms for other individuals who could not lawfully obtain the firearms. Based on my training and experience, individuals involved in the conspiracy will communicate through cellular telephones, such as the Device, to further their conspiracy. Accordingly, there is probable cause to believe that there is evidence, and instrumentalities of conspiring to make false statements to federally licensed firearm dealers in violation of 18 U.S.C. §§ 922(a)(6) & 371 on the Device.

23. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of ATF.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice

communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my training, experience, I know that the Device has capabilities that allow it to serve all or some of the following functions: wireless telephone, a digital camera, portable media player, GPS navigation device, and accessing / downloading information from the Internet. Electronic devices can store information for long periods of time. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence of a crime

and it can also reveal or suggest who possessed or used the Device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how

a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property ("Device") to be searched is White and Rose color Apple iPhone model A1586 with IMEI 356153092554788 and currently in the custody of ATF. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that are evidence or instrumentalities of violations of 18 U.S.C. §§ 922(a)(6), 922(g)(3), and 371, including but not limited to:

a. Texts, voicemails, emails or any electronic communications;

b. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium;

2. Any and all information, notes, software, documents, records, or correspondence, in any format and medium.

3. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted with the Device or by other means.

4. The list of all telephone calls made or received located in the memory of the Device.

5. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.